OIPE IAP47
JAN 17 2006
PATENT & TRADEMARK OFFICE

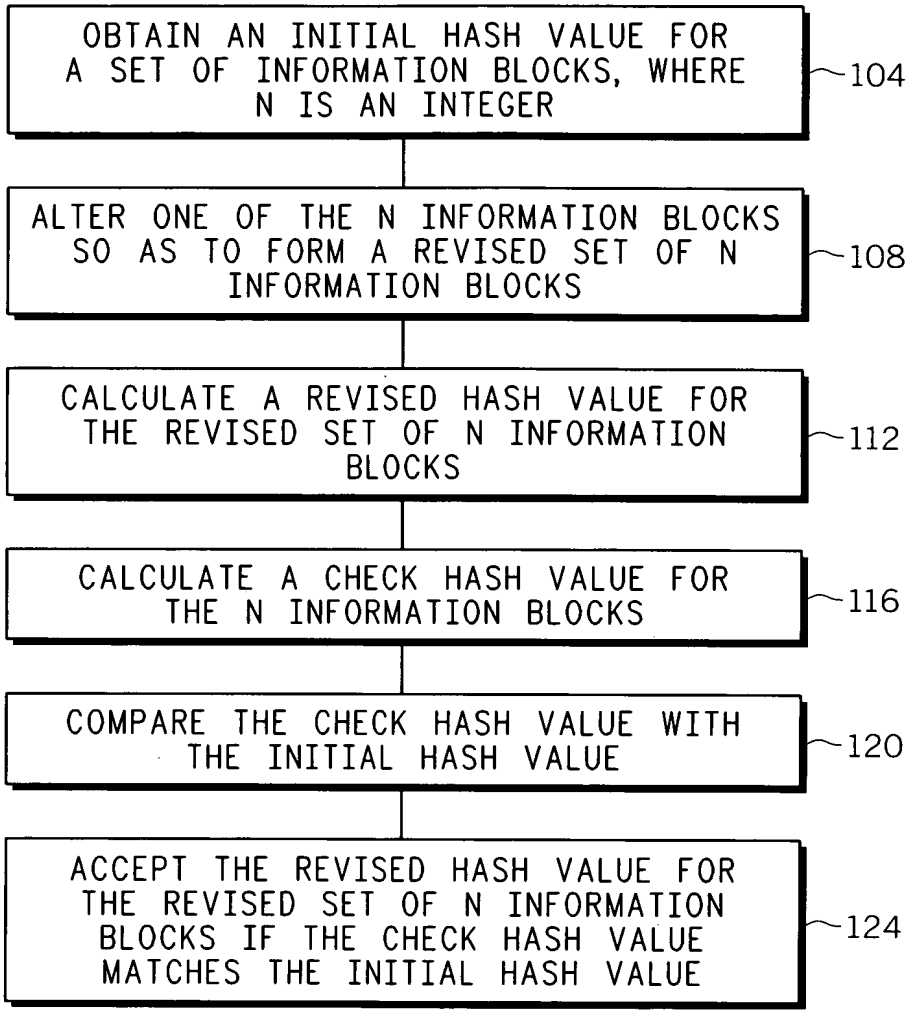


FIG. 1

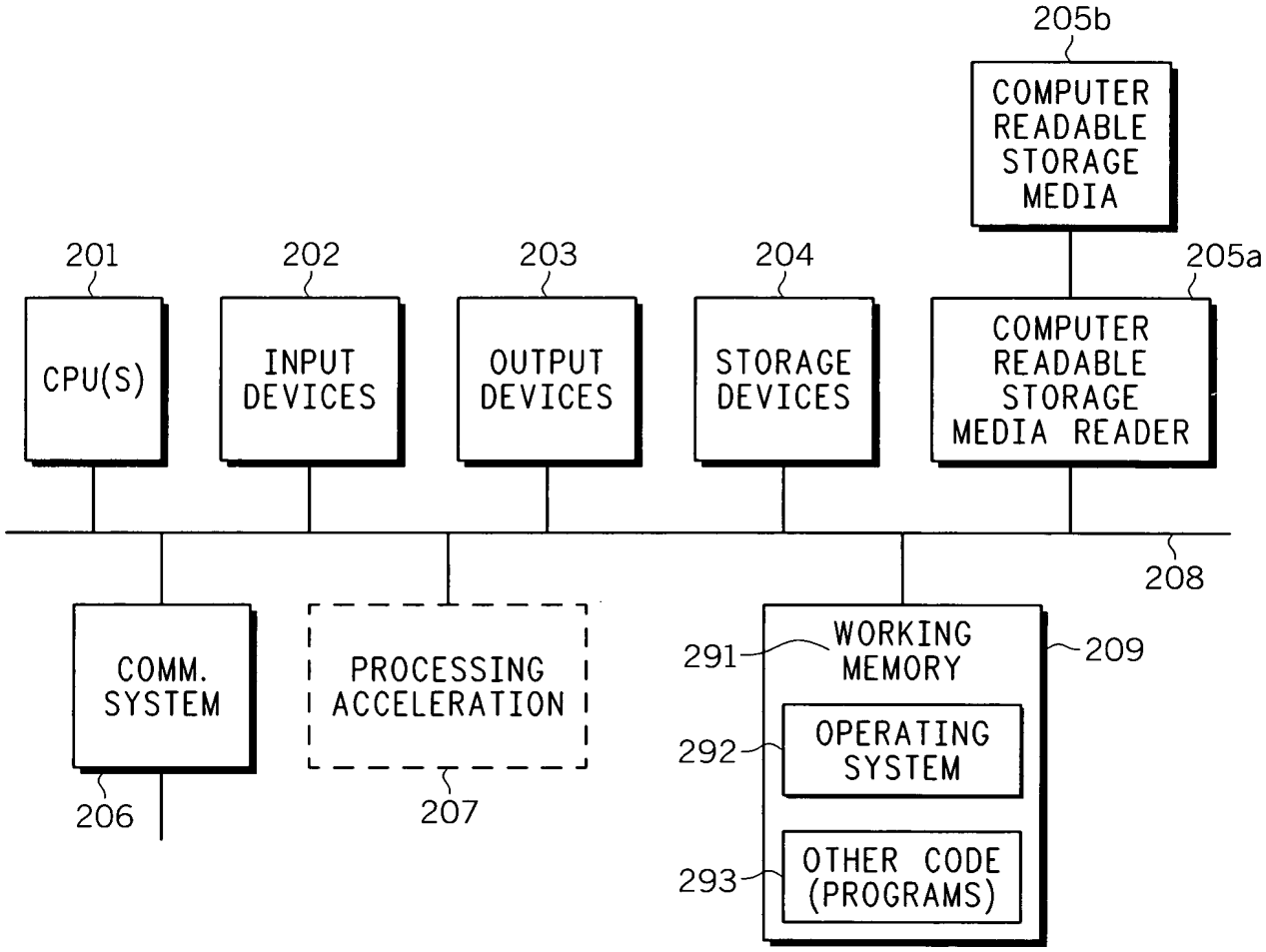
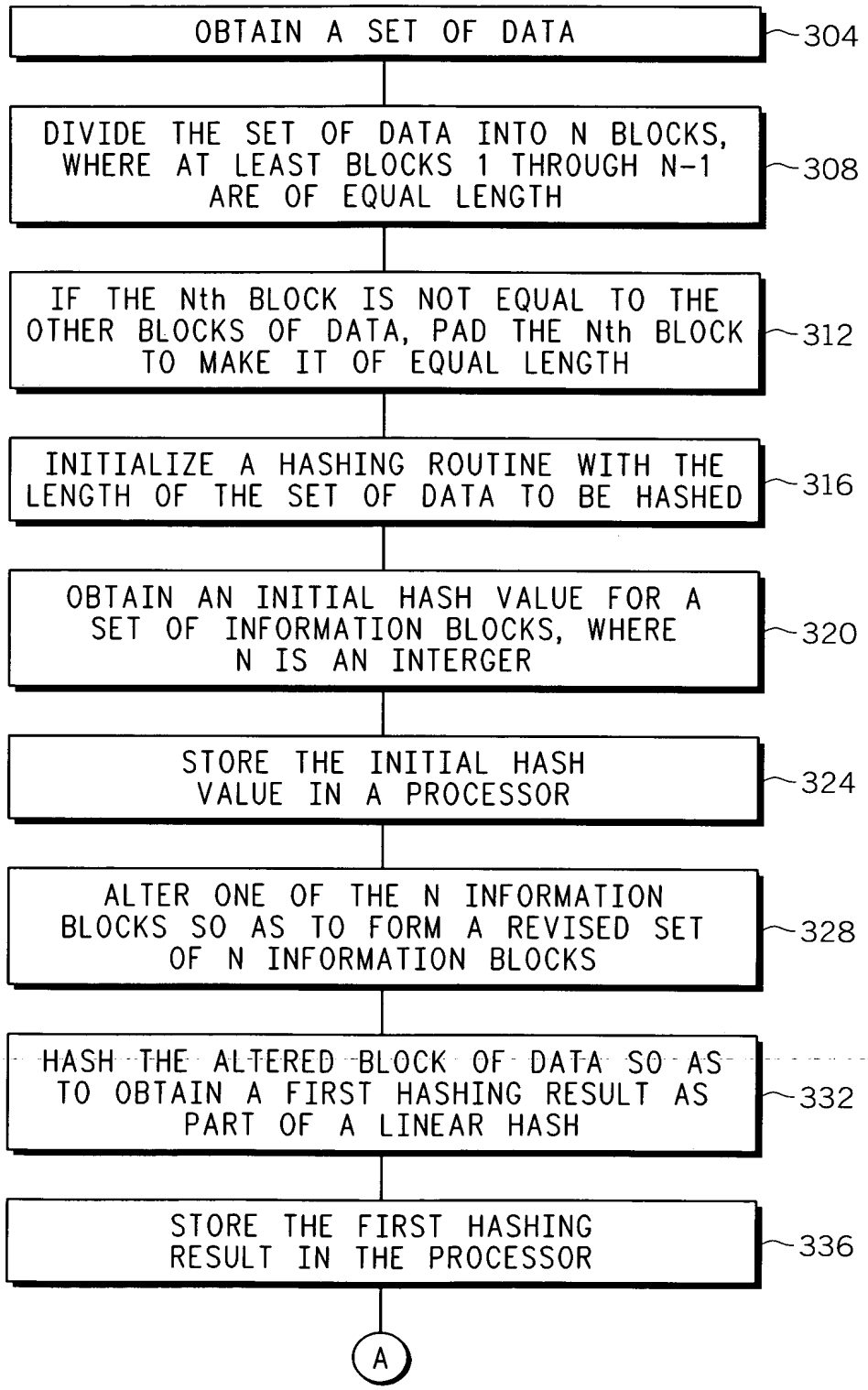

205b
COMPUTER READABLE STORAGE MEDIA
201
202
203
204
205a
CPU(S)
INPUT DEVICES
OUTPUT DEVICES
STORAGE DEVICES
COMPUTER READABLE STORAGE MEDIA READER
208
COMM. SYSTEM
PROCESSING ACCELERATION
291
WORKING MEMORY
209
292
OPERATING SYSTEM
293
OTHER CODE (PROGRAMS)
206
207
200

FIG. 2


OBTAIN A SET OF DATA
304
DIVIDE THE SET OF DATA INTO N BLOCKS, WHERE AT LEAST BLOCKS 1 THROUGH N-1 ARE OF EQUAL LENGTH
308
IF THE Nth BLOCK IS NOT EQUAL TO THE OTHER BLOCKS OF DATA, PAD THE Nth BLOCK TO MAKE IT OF EQUAL LENGTH
312
INITIALIZE A HASHING ROUTINE WITH THE LENGTH OF THE SET OF DATA TO BE HASHED
316
OBTAIN AN INITIAL HASH VALUE FOR A SET OF INFORMATION BLOCKS, WHERE N IS AN INTERGER
320
STORE THE INITIAL HASH VALUE IN A PROCESSOR
324
ALTER ONE OF THE N INFORMATION BLOCKS SO AS TO FORM A REVISED SET OF N INFORMATION BLOCKS
328
HASH THE ALTERED BLOCK OF DATA SO AS TO OBTAIN A FIRST HASHING RESULT AS PART OF A LINEAR HASH
332
STORE THE FIRST HASHING RESULT IN THE PROCESSOR
336
A

300

FIG. 3A

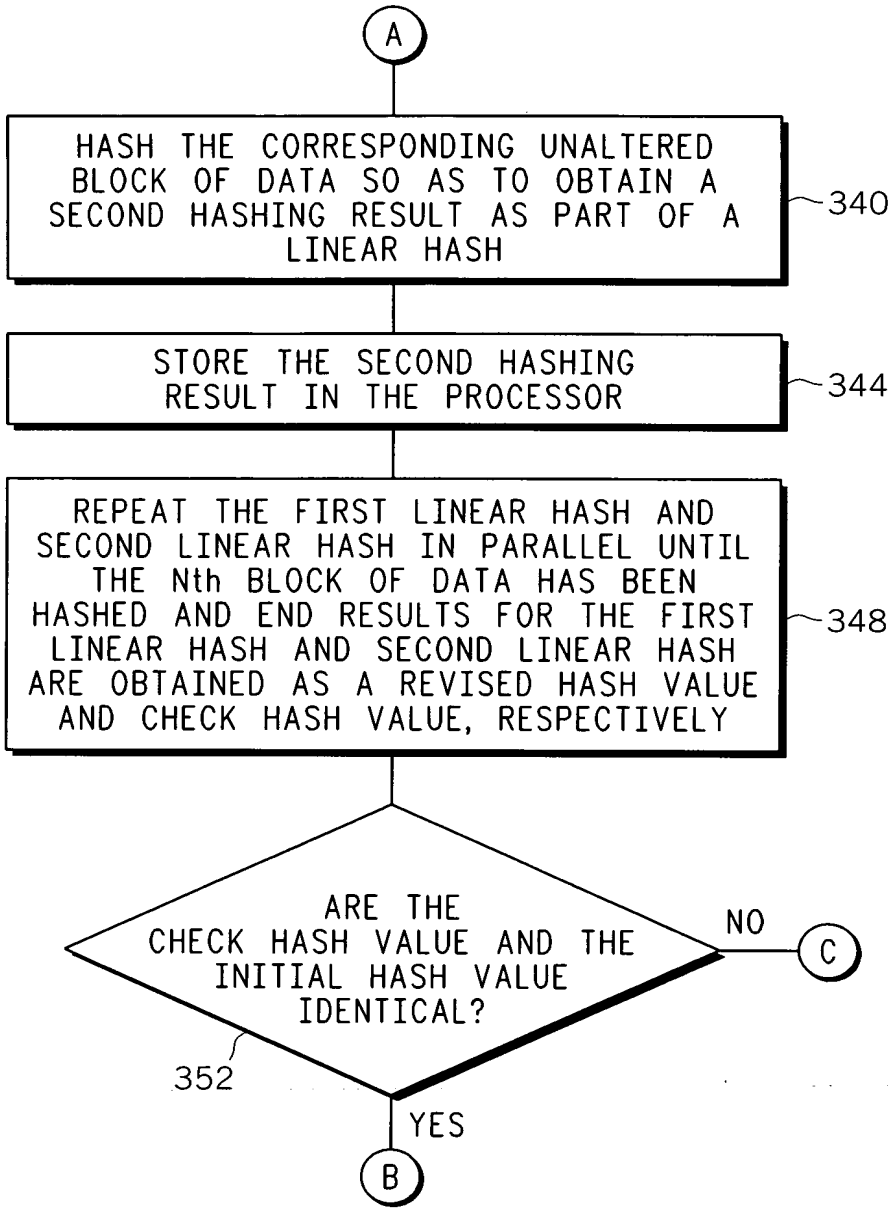

A
HASH THE CORRESPONDING UNALTERED BLOCK OF DATA SO AS TO OBTAIN A SECOND HASHING RESULT AS PART OF A LINEAR HASH
340
STORE THE SECOND HASHING RESULT IN THE PROCESSOR
344
REPEAT THE FIRST LINEAR HASH AND SECOND LINEAR HASH IN PARALLEL UNTIL THE Nth BLOCK OF DATA HAS BEEN HASHED AND END RESULTS FOR THE FIRST LINEAR HASH AND SECOND LINEAR HASH ARE OBTAINED AS A REVISED HASH VALUE AND CHECK HASH VALUE, RESPECTIVELY
348
ARE THE CHECK HASH VALUE AND THE INITIAL HASH VALUE IDENTICAL?
352
NO
C
YES
B

FIG. 3B

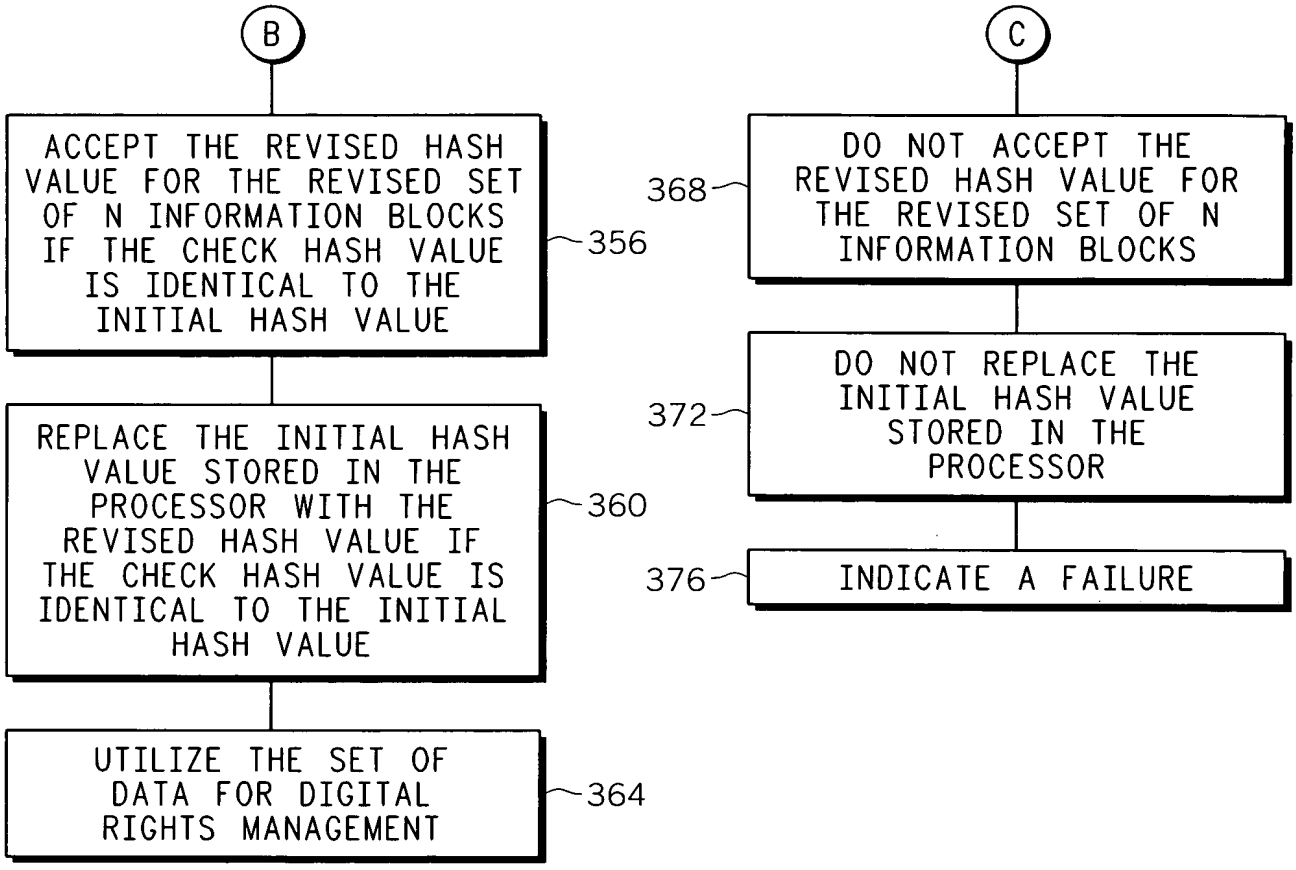

B
ACCEPT THE REVISED HASH VALUE FOR THE REVISED SET OF N INFORMATION BLOCKS IF THE CHECK HASH VALUE IS IDENTICAL TO THE INITIAL HASH VALUE
356
REPLACE THE INITIAL HASH VALUE STORED IN THE PROCESSOR WITH THE REVISED HASH VALUE IF THE CHECK HASH VALUE IS IDENTICAL TO THE INITIAL HASH VALUE
360
UTILIZE THE SET OF DATA FOR DIGITAL RIGHTS MANAGEMENT
364
C
368
DO NOT ACCEPT THE REVISED HASH VALUE FOR THE REVISED SET OF N INFORMATION BLOCKS
372
DO NOT REPLACE THE INITIAL HASH VALUE STORED IN THE PROCESSOR
376
INDICATE A FAILURE

FIG. 3C

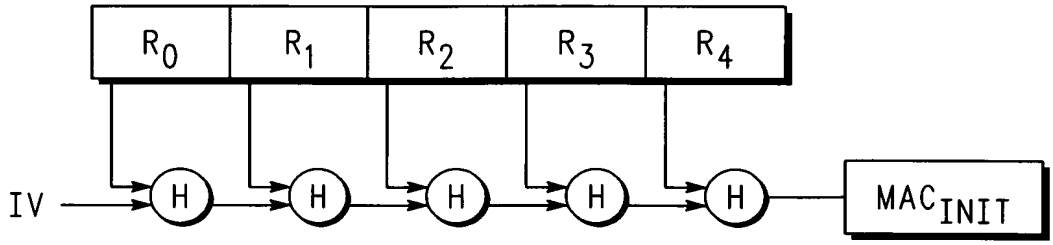

R0
R1
R2
R3
R4
IV
H
H
H
H
H
MACINIT

FIG. 4A

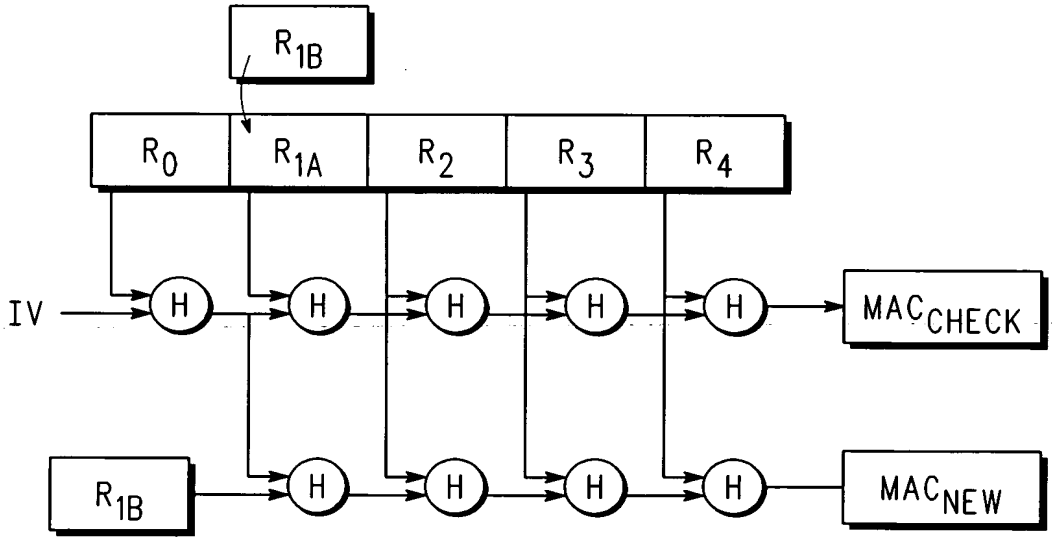

R1B
R0
R1A
R2
R3
R4
IV
H
H
H
H
H
MACCHECK
R1B
H
H
H
H
MACNEW

FIG. 4B

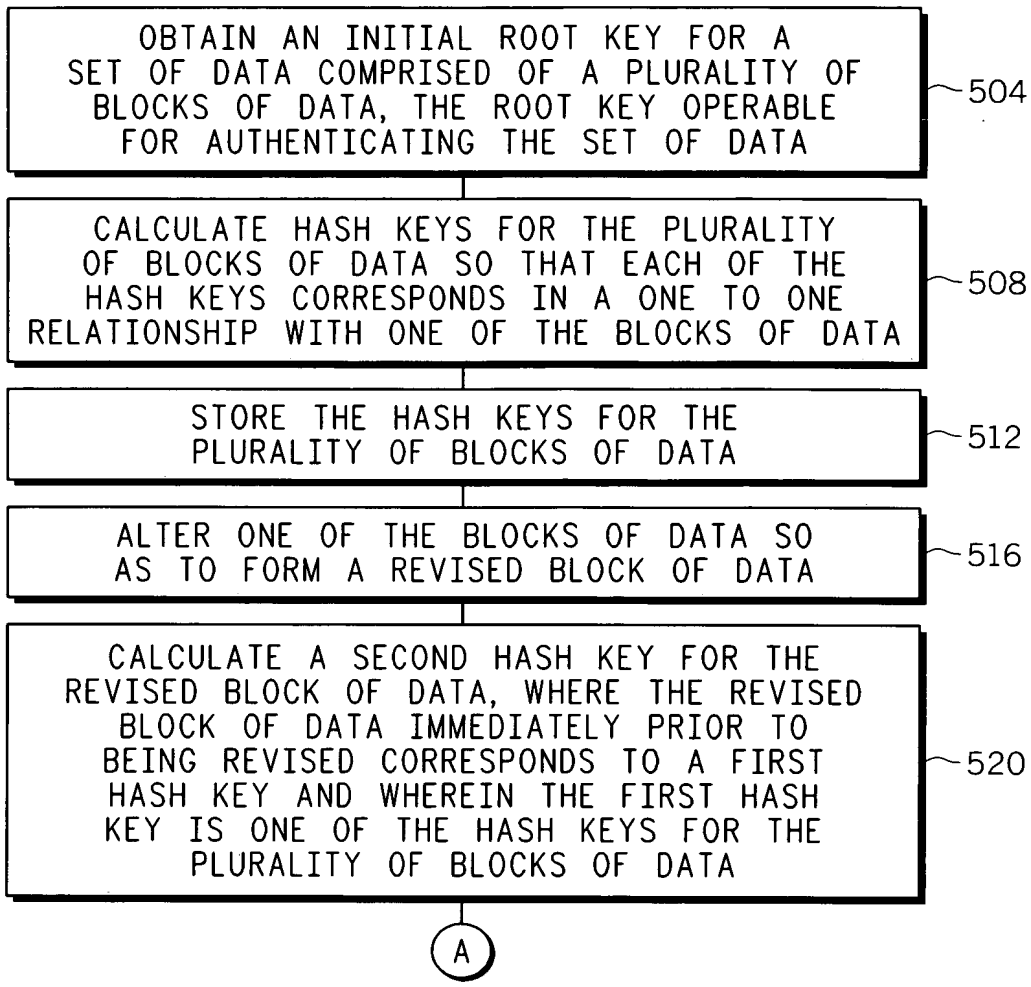
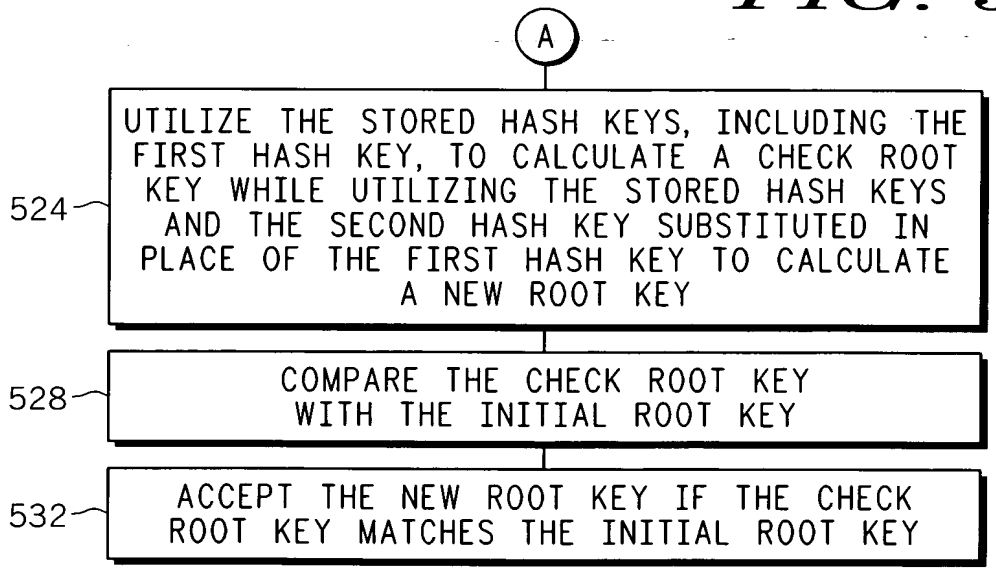


FIG. 5A

500

FIG. 5B



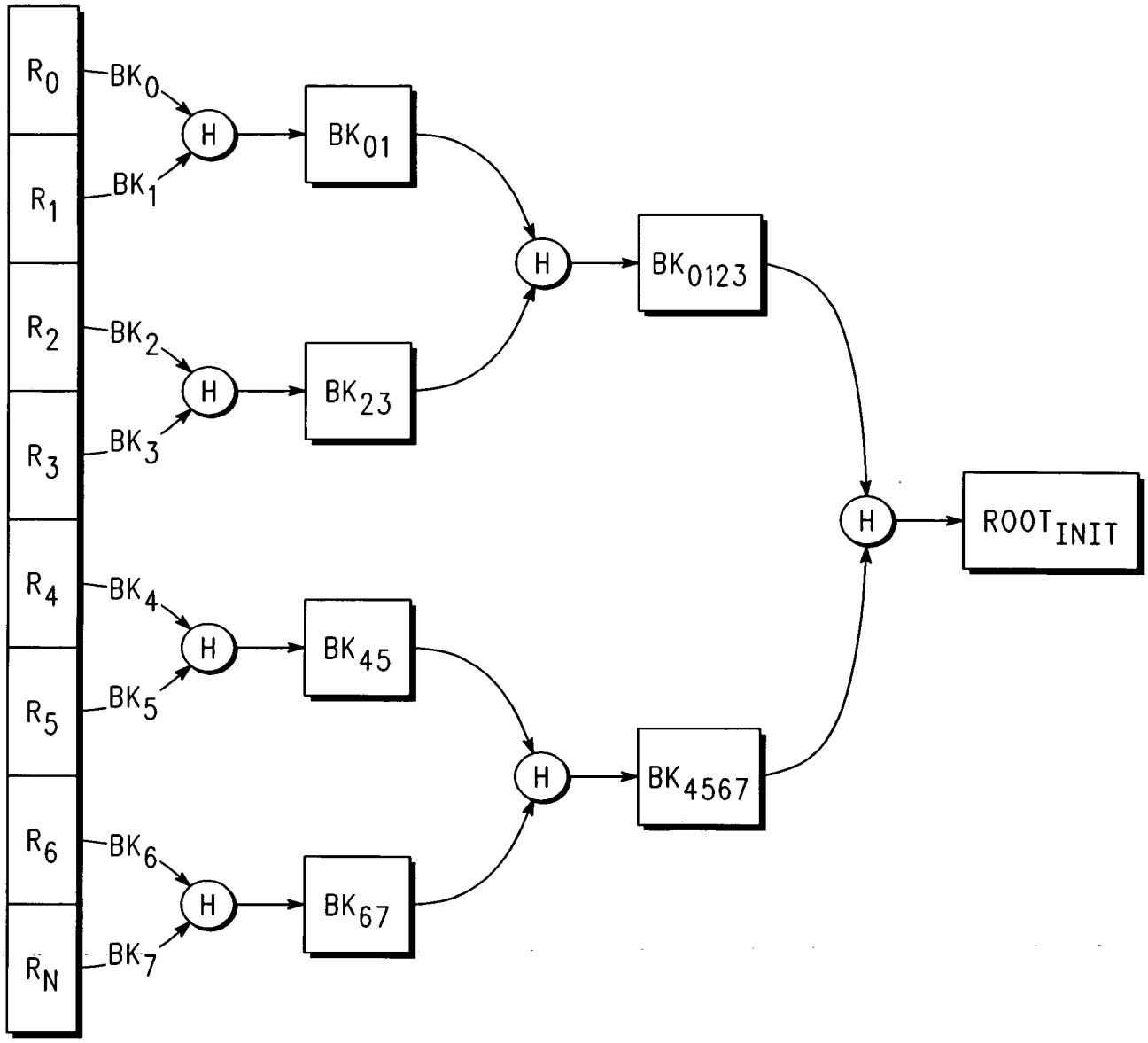

R0
R1
R2
R3
R4
R5
R6
RN
BK0
BK1
BK2
BK3
BK4
BK5
BK6
BK7
H
BK01
BK23
BK45
BK67
BK0123
BK4567
ROOTINIT

FIG. 6

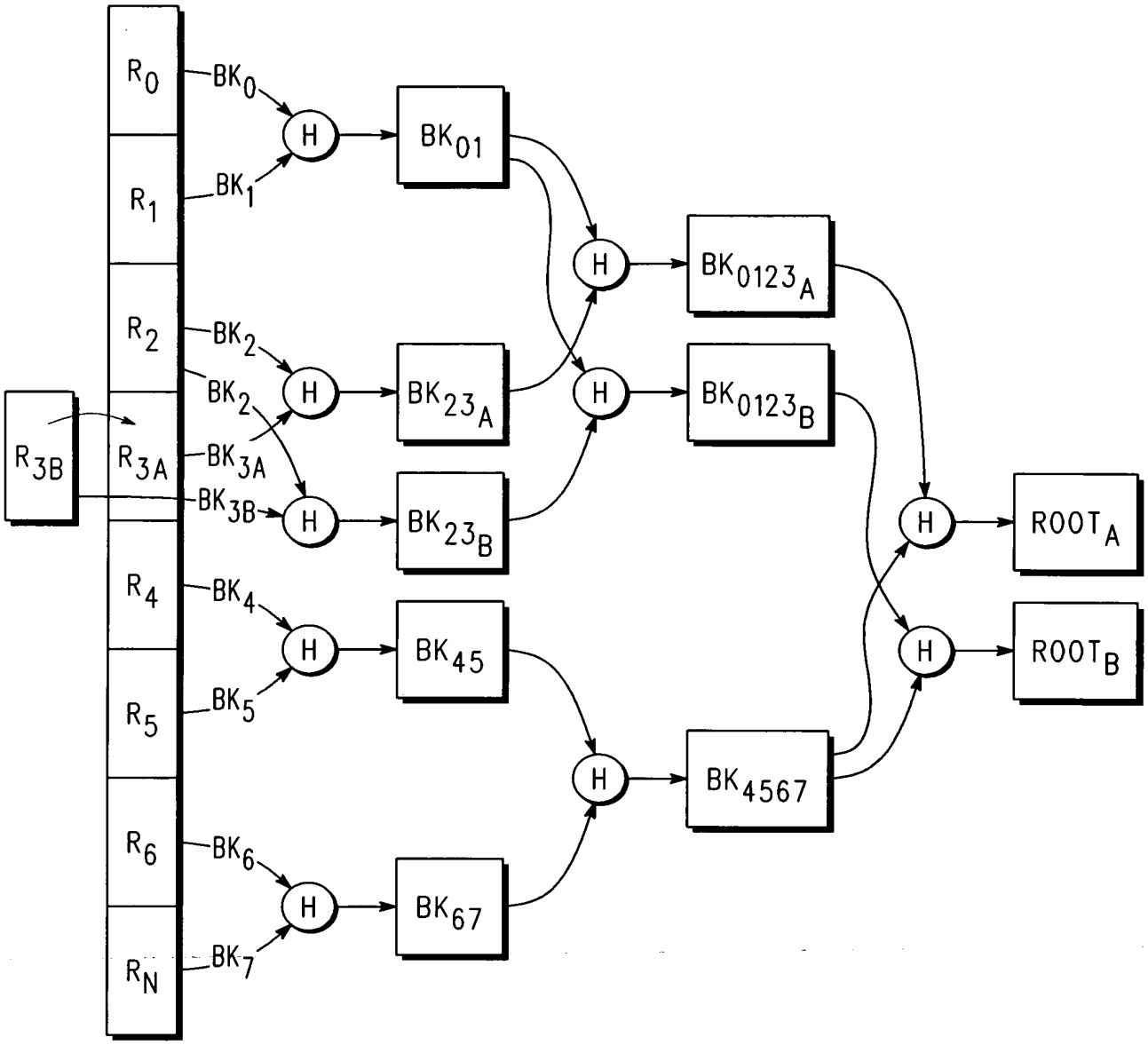
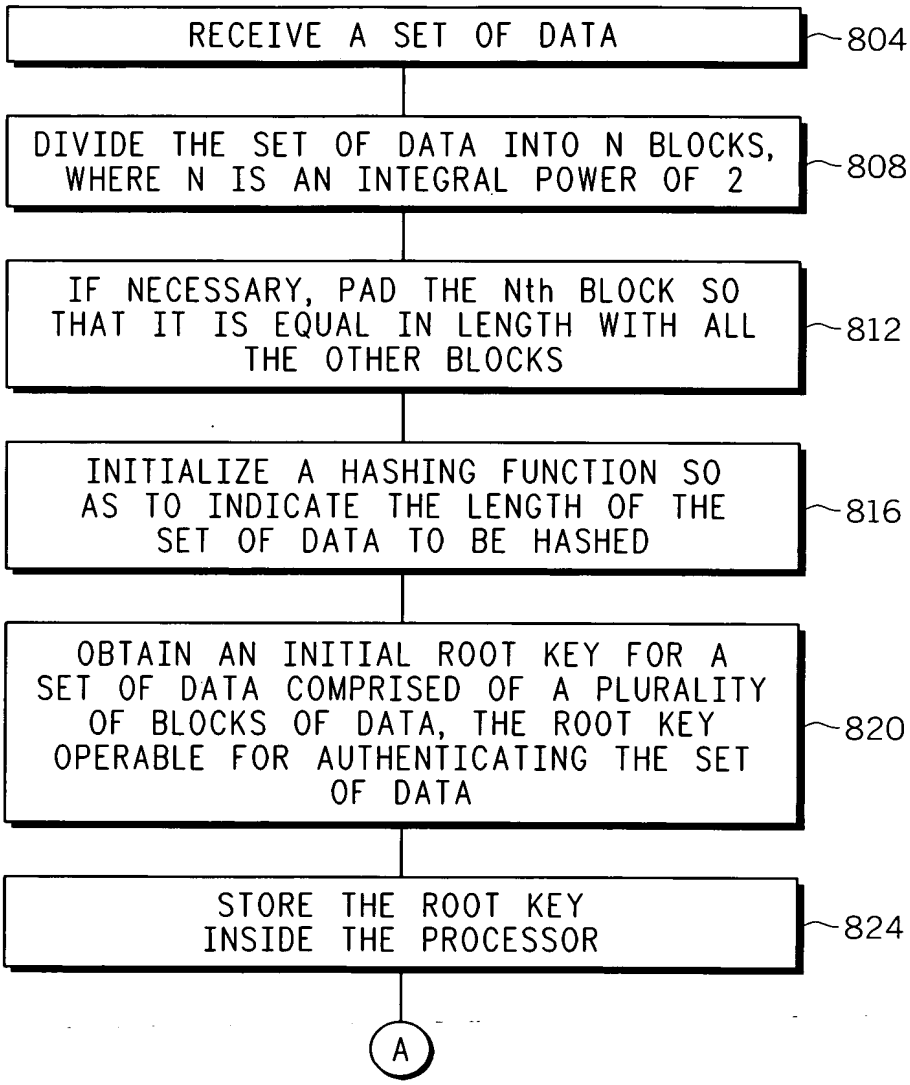

R0
R1
R2
R3B
R3A
R4
R5
R6
RN
BK0
BK1
BK2
BK2
BK3A
BK3B
BK4
BK5
BK6
BK7
H
BK01
BK23A
BK23B
BK45
BK67
BK0123A
BK0123B
BK4567
ROOTA
ROOTB

FIG. 7


RECEIVE A SET OF DATA
804
DIVIDE THE SET OF DATA INTO N BLOCKS, WHERE N IS AN INTEGRAL POWER OF 2
808
IF NECESSARY, PAD THE Nth BLOCK SO THAT IT IS EQUAL IN LENGTH WITH ALL THE OTHER BLOCKS
812
INITIALIZE A HASHING FUNCTION SO AS TO INDICATE THE LENGTH OF THE SET OF DATA TO BE HASHED
816
OBTAIN AN INITIAL ROOT KEY FOR A SET OF DATA COMPRISED OF A PLURALITY OF BLOCKS OF DATA, THE ROOT KEY OPERABLE FOR AUTHENTICATING THE SET OF DATA
820
STORE THE ROOT KEY INSIDE THE PROCESSOR
824
A

800

FIG. 8A

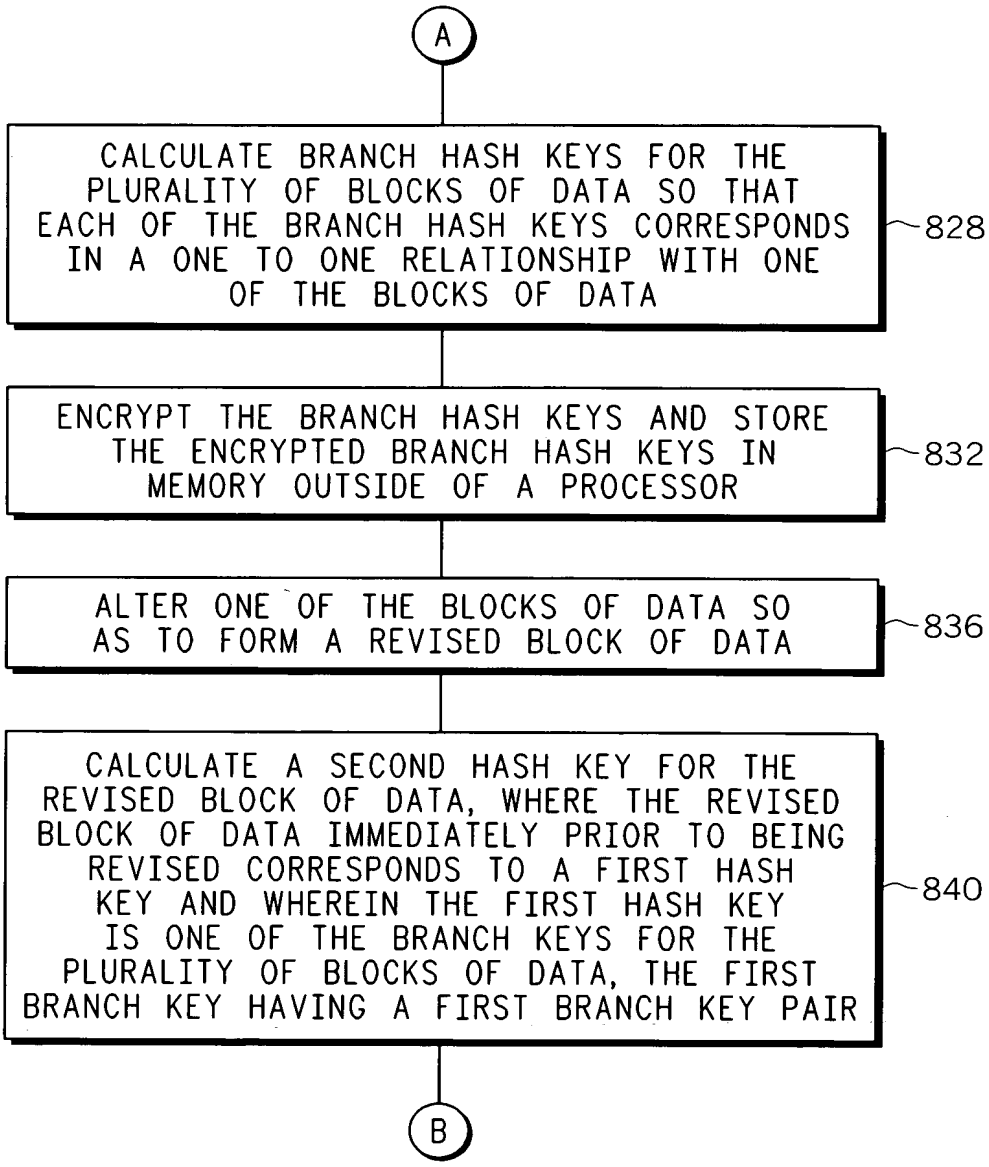

A
CALCULATE BRANCH HASH KEYS FOR THE PLURALITY OF BLOCKS OF DATA SO THAT EACH OF THE BRANCH HASH KEYS CORRESPONDS IN A ONE TO ONE RELATIONSHIP WITH ONE OF THE BLOCKS OF DATA
828
ENCRYPT THE BRANCH HASH KEYS AND STORE THE ENCRYPTED BRANCH HASH KEYS IN MEMORY OUTSIDE OF A PROCESSOR
832
ALTER ONE OF THE BLOCKS OF DATA SO AS TO FORM A REVISED BLOCK OF DATA
836
CALCULATE A SECOND HASH KEY FOR THE REVISED BLOCK OF DATA, WHERE THE REVISED BLOCK OF DATA IMMEDIATELY PRIOR TO BEING REVISED CORRESPONDS TO A FIRST HASH KEY AND WHEREIN THE FIRST HASH KEY IS ONE OF THE BRANCH KEYS FOR THE PLURALITY OF BLOCKS OF DATA, THE FIRST BRANCH KEY HAVING A FIRST BRANCH KEY PAIR
840
B

FIG. 8B

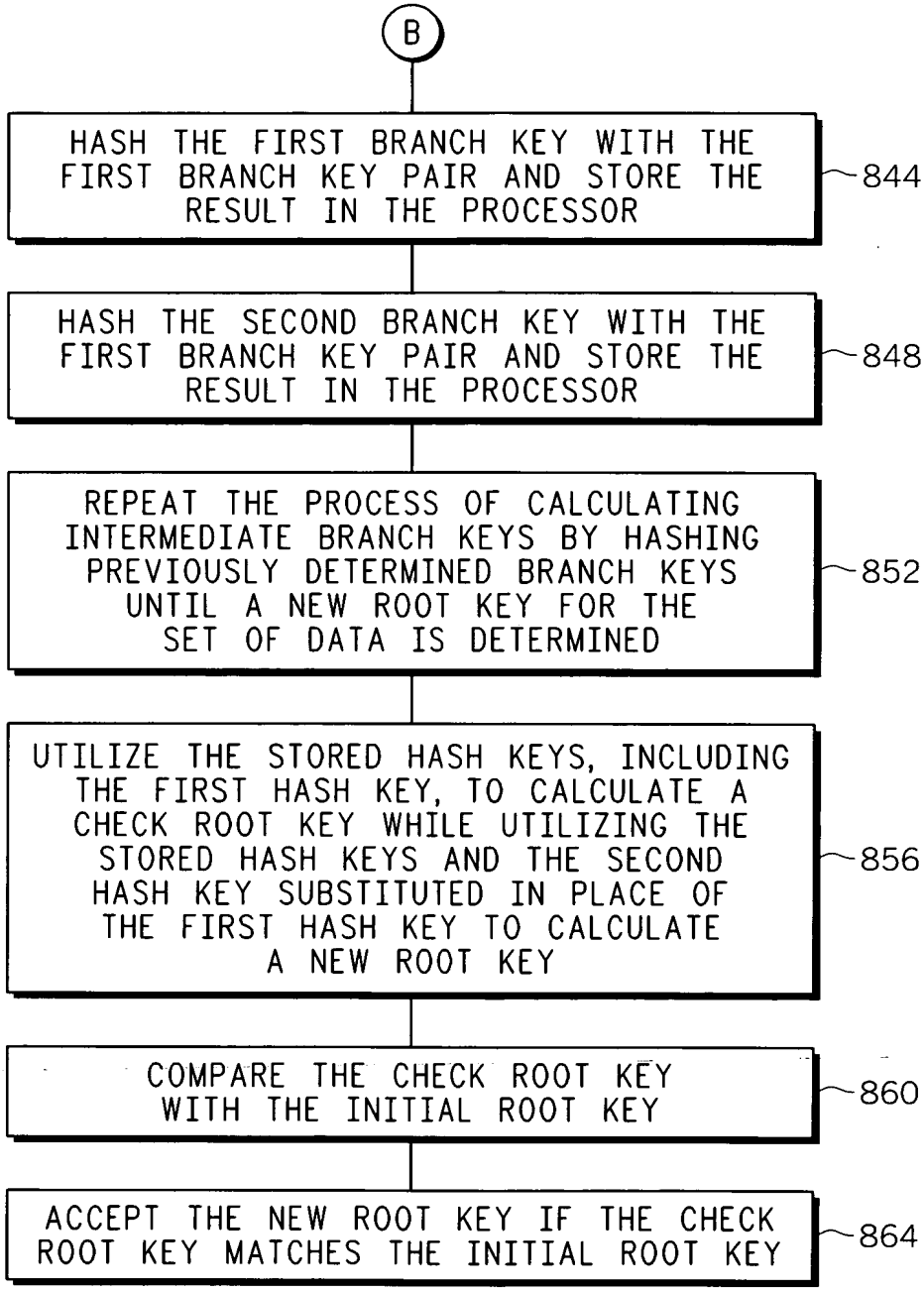

B
HASH THE FIRST BRANCH KEY WITH THE FIRST BRANCH KEY PAIR AND STORE THE RESULT IN THE PROCESSOR
844
HASH THE SECOND BRANCH KEY WITH THE FIRST BRANCH KEY PAIR AND STORE THE RESULT IN THE PROCESSOR
848
REPEAT THE PROCESS OF CALCULATING INTERMEDIATE BRANCH KEYS BY HASHING PREVIOUSLY DETERMINED BRANCH KEYS UNTIL A NEW ROOT KEY FOR THE SET OF DATA IS DETERMINED
852
UTILIZE THE STORED HASH KEYS, INCLUDING THE FIRST HASH KEY, TO CALCULATE A CHECK ROOT KEY WHILE UTILIZING THE STORED HASH KEYS AND THE SECOND HASH KEY SUBSTITUTED IN PLACE OF THE FIRST HASH KEY TO CALCULATE A NEW ROOT KEY
856
COMPARE THE CHECK ROOT KEY WITH THE INITIAL ROOT KEY
860
ACCEPT THE NEW ROOT KEY IF THE CHECK ROOT KEY MATCHES THE INITIAL ROOT KEY
864

FIG. 8C